International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 21st Sept2017. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-8

Title: **CIRCUIT POLICY ATTRIBUTE-BASED VERIFIABLE DELEGATION IN CLOUD COMPUTING**

Volume 06, Issue 08, Pages: 280– 286.
Paper Authors

T.CHENNA REDDY, M VENKATESH NAIK , DR.G.PRAKASH BABU
St Mark Educational institution society group of institution, AP..

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CIRCUIT POLICY ATTRIBUTE-BASED VERIFIABLE DELEGATION IN CLOUD COMPUTING

T.CHENNA REDDY[1], M VENKATESH NAIK[2] , DR.G.PRAKASH BABU[3]

[1]PG Scholar, CSE, St Mark Educational institution society group of institution, AP.
[2]Assistant Professor, CSE, St Mark Educational institution society group of institution, AP.
[3]Professor, CSE, St Mark Educational institution society group of institution, AP.

ABSTRACT: In the cloud, for achieving access control and data security, the data owners could uses attribute-based encryption to encrypt the stored data. To reduce the cost, the users which has a limited computing power are nevertheless more likely to delegate the mask of the decryption task to the cloud servers. The result shows, attribute based encryption with delegation come out. Still, there are some problems and questions regarding to previous related works. For example, during the delegation or release, the cloud servers could misrepresent or replace the delegated ciphertext and respond a fake result with malevolent intent. As well as for the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible during the encryption. Since policy for general circuits are used to achieve the strongest form of access control, a construction to design circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been developed. This system is mixed with verifiable computation and encrypt-then-Mac mechanism, the data confidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time. As well as this scheme achieves security against chosen-plaintext attacks under the multilinear Decisional DiffieHellman assumption. Moreover, this scheme achieves feasibility as well as efficiency.

KEYWORDS: Ciphertext-policy attribute-based encryption, circuits, verifiable delegation, multi linear map, hybrid encryption.

I. INTRODUCTION

Cloud computing is innovation which uses advanced computational power as well as improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. The advantage of cloud is cost savings. The prime disadvantage is security. The appearance of cloud computing transports a radical novelty to the organization of the data possessions within this calculating surroundings, the cloud servers can present different data services, such as isolated data storage and outsourced allocation calculation etc. For information cargo space, the servers amass a huge quantity of communal information, which might be

accessed by certified users. For allocation calculation, the servers could be accustomed to hold and determine frequent data dealing to the user's burden. As applications shift to cloud computing proposals, verifying delegation process using cipher text-policy attribute-based encryption (CP-ABE) is used to guarantee the data privacy and the verifiability of allocation on untruthful cloud servers. Captivating health check data distribution as an example among the rising volumes of health check images and health check records, the medical care associations set a big amount of data in the cloud for dropping. To make such data sharing be achievable, attribute based encryption is used. There are two forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the second is ciphertext-policy attribute-based encryption. In CP-ABE system, each ciphertext is contains an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if and only if the key's attribute set satisfies the access structure associated with a ciphertext. The cloud server provides another service which is delegation computing.The VD-CPABE schemeshows that the untrusted cloud will not be able to learn anything about the encrypted message and build the original ciphertext.

2 RELATED WORKS:

Outsourcing Decryption of Multi-Authority ABE Cipher texts Keying Li and Hue Ma

The believed of multi-authority attribute established encryption was gave by Pursue in TCC 2007. In this paper, we enhance Chase's scheme to permit encryptions to ascertain how countless qualities are needed for every single ciphertext from connected attribute authorities. The counseled scheme can be perceived as a multi-trapdoor construction. Further-more, we apply the LMSSS to outsource the decryption of multi-authority attribute established encryption scheme for colossal universe. Also, the outsourcing scheme can be comprehended in the setting of multi-authority key-policy attribute established encryption. Both our schemes can be spread to RCCA safeguard ones. Attribute Instituted Encryption alongside Privacy Maintaining employing Asymmetric Key in Cloud Computing S.Sankareswar and S.Hemanth Symmetric key algorithm uses alike key for both encryption and decryption. The authors seize a centralized way whereas a solitary key allocation center (KDC) distributes hidden keys and qualities to all users. A new decentralized admission manipulation scheme for safeguard data storage in clouds that supports nameless authentication. The validity of the user who stores the data is additionally verified. The counseled scheme is to obscure the users qualities employing SHA algorithm .The Parlier cryptosystem, is a probabilistic asymmetric algorithm for area key cryptography. Parlier algorithm use for Conception of admission strategy, file accessing and file refubishing procedure and additionally obscuring the admission strategy to the user employing query established algorithm.

Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and

Provably Safeguard Realization Brent Waters 2006 We present a new methodology for comprehending Ciphertext-Policy Attribute Encryption (CP-ABE) below concrete and non-interactive cryptographic assumptions in the average model. Our resolutions permit each encrypt or to enumerate admission manipulation in words of each admission formula above the qualities in the system. In our most effectual arrangement, ciphertext size, Encryption and decryption period scales linearly alongside the intricacy of the admission formula. The merely preceding work to accomplish these parameters was manipulated to a facts in the generic cluster model. We present three constructions inside our framework. Our arrangement is proven selectively safeguard below an assumption that we call the decisional Parallel Bilinear Die-Hellman Exponent (PBDHE) assumption that can be believed as a generalization of the BDHE assumption. Our subsequent two constructions furnish presentation transactions to accomplish provable protection suitably below the (weaker) decisional Bilinear-Di e-Hellman Exponent and decisional Bilinear Die-Hellman assumptions. How to Representative and Confirm in Public: Verifiable Computation from Attribute-based Encryption Bryan Par no Mariana Beam ova and Vend Vaikuntanathan 2011 The expansive collection of tiny, computationally frail mechanisms and the producing number of computationally intensive tasks makes it appealing to representative computation to data centers. Though, outsourcing computation is functional merely after the returned consequence can be trusted, which Makes verifiable computation (VC) a have to for such scenarios. In this work we spread the meaning of verifiable computation in two vital directions: area delegation and area verifiability, that have vital requests in countless useful delegation scenarios. Yet, continuing VC constructions established on average cryptographic assumptions flounder to accomplish these properties Cryptanalysis of the Multilinear Chart above the Integers Jung He Chon, Kyoohyung Han and Altering Lee 2014.

3 PRELIMINARY

A.Our Contribution

Existing system in every ciphertext is related to associate degree access structure, and every non -public secret is labeled with a group of descriptive attributes. A user is in a position to rewrite a ciphertext if the key's attribute set satisfies the access structure related to a ciphertext. CP -ABE below sure access policies. The users, UN agency wish to access the information files, select to not handle the complicated method of decoding domestically as a result of restricted resources. Instead, they're presumably to source a part of the decoding method to the cloud server. whereas the untrusted cloud servers UN agency will translate the first ciphertext into a straightforward one may learn nothing concerning the plaintext fro m the delegation. whereas the untrusted cloud servers UN agency will translate the first ciphertext into a straightforward one may learn nothing concerning the plaintext fro m the delegation.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

B.Our Techniques

The increasing volumes of records place an outsized quantity information of knowledge of information within the cloud for reducing information storage prices and supporting data cooperation. every cipher text is related to associate degree access structure and user is ready to decipher a cipher text, the storage service provided by the cloud server and therefore the outsourced information[4] mustn't be leaked even though malware or hackers infiltrate the server. User may validate whether or not the cloud server responds correct remodeled cipher text to assist him/her decipher cipher text straight off and properly

4 . SYSTEM ARCHITECTURE

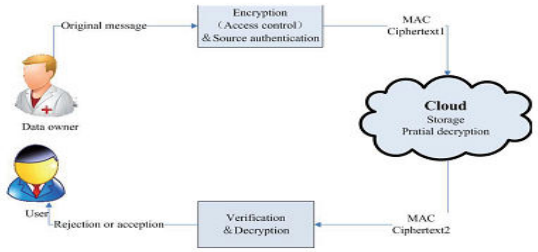

Fig.1. SYSTEM ARCHITECTURE

A. MODULES

Attribute Authority

Cloud Server

Data owner

Data Consumer

1. Attribute Authority Authority will have to provide the key, as per the user's key request. Every users request will have to be raised to authority to get access key on mail. There are two complementary forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CPABE). In a KP-ABE system, the decision of access policy is made by the key distributor instead of the enciphered, which limits the practicability and usability for the system in practical applications.

2. Cloud Server Cloud server will have the access to files which are uploaded by the data owner Cloud server needs to decrypt the files available under their permission. Furthermore data user will have to decrypt the data to access the original text by providing the respective key. File has been decrypted successfully and provided for consumer.

3. Data Owner Data owner will have to register initially to get access to the profile. Data Owner will upload the file to the cloud server in the encrypted format. Random encryption key generation is happening while uploading the file to the cloud. Encrypted file will be stored on the cloud.

4. Data Consumer Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data consumer can access the file based on the key received from mail id. As per the key received the consumer can verify and decrypt the data from the cloud.

5. PROPOSED SYSTEM

Attribute-based encryption the notion of attribute-based encryption (ABE). In subsequent works, they focused on policies across multiple authorities and the issue of what expressions they could achieve. Up until recently, raised a construction for realizing KPABE for general circuits. Prior to this method, the strongest form of expression is Boolean formulas in ABE systems, which is still a far cry from being

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

able to express access control in the form of any program or circuit. Actually, there still remain two problems. The first one is their have no construction for realizing CPABE for general circuits, which is conceptually closer to traditional access control. The other is related to the efficiency, since the exiting circuit ABE scheme is just a bit encryption one. Thus, it is apparently still remains a pivotal open problem to design an efficient circuit CP-ABE scheme. Hybrid encryption the generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length. Based on their ingenious work, a one-time MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption. Such improved model has the advantage of achieving higher security requirements. ABE with Verifiable Delegation. Since the introduction of ABE, there have been advances in multiple directions. The application of outsourcing computation is one of an important direction. The first ABE with outsourced decryption scheme to reduce the computation cost during decryption. The definition of ABE with verifiable outsourced decryption. They seek to guarantee the correctness of the original cipher text by using a commitment. However, since the data owner generates a commitment without any secret value about his identity, the un trusted server can then forge a commitment for a message he chooses. Thus the cipher text relating to the message is at risk of being tampered. Furthermore, just modify the commitments for the cipher text relating to the message is not enough. The cloud server can deceive the user with proper permissions by responding the terminator $\perp$ to cheat that he/she is not allowed to access to the data.

A. Notations Zp - finite field with prime order p. $\perp$ - formal symbol denotes termination. $x \leftarrow X$- x is randomly selected from X. A is an algorithm then $A(x) \rightarrow y$ denotes that y is the output by running the algorithm A on input x. $G(\lambda, k)$- group generation algorithm where λ is the security Parameter. k -the number of allowed pairing operation. ε: $Zp \rightarrow R$- *negligible* if for every $c > 0$ there is a K such that $\varepsilon(k) < k-c$ for all $k > K$.

B. Algorithms Used Following are few other algorithms which are used:

1. Setup(λ, n, l) This algorithm is executed by the authority. It takes as input a security parameter λ, the number n of input size and the maximum depth l of a circuit. $PK = (g\_ k, H1, H2, H3, y, h1, ..., hn, hn+1, ..., h2n)$, $MK = g\_$. *2) Hybrid-encrypt* $(PK, f = (n, q, A, B, GateType), M \in \{0, 1\}m)$): This algorithm is executed by the data owner. Taking the public parameters PK, a description f of a circuit and a message $M \in \{0, 1\}m$ as input.

2. KeyGen(MK, x ∈ {0, 1}n) The authority generates the private key for the user. Then the user sends his transformation key to the cloud server. This algorithm takes as input the master secret key and a description of the attribute $x \in \{0, 1\}n$. It firstly chooses a random $t \in Zp$. Then it creates the private key as $KH = g\_yt$, $L = gt$, if $xi = 1$ $Ki = (yhi)t$, if $xi = 0$ $Ki = (yhn+i)t$, $i \in [1, n]$. The transformation key is $TK = \{L, Ki, i \in [1, n]\}$.Note that, for the data owner IDo, the authority generates his private key with the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

identity attribute *ID*0 as *KH* = *g_yt*, *L* = *gt*, *KIDo* = *Ht*3 (*IDo*).

3. Transform(TK,CT)

The transformation algorithm is executed by the cloud server. It takes as input the transformation key *TK* and the original ciphertext *CT*. The algorithm partially decrypts the ciphertext.

C. Design Goals For effective utilization of outsourced data, our system should achieve security and performance guarantee as follows:

1. Secure Keyword Search To explore different mechanisms for designing effective keyword search schemes based on the existing searchable encryption framework.

2. Secure Data Sharing To allow user to share data over the cloud without losing privacy.

3. Security Guarantee To prevent cloud server from learning the plaintext of either the data files or the searched keywords, and achieve the as strong- as- possible security strength compared to existing searchable encryption schemes.

4. Efficiency Above goals should be achieved with minimum communication and computation overhead.

6. CONCLUSION

In the cloud, for accomplished admission association and keeping vision confidential, the knowledge the info the information homeowners could accept attribute-based cryptography to encipher the grasp on data. decoding task to the cloud servers to cut back the computing value. Our ciphertext strategy attribute - based hybrid cryptography, we incline to could representative the verifiable partial decoding to the cloud server

7 REFERENCES

[1]M. Armbrust, A. Fo x, R. Griffith, A. D. Joseph, R. H. Kat z, A.Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M.Zaharia , ”Above the Clouds: A Berkeley View of Cloud Co mputing, “Un iversity of California, Berkeley, Technical Report, no. UCB/EECS -2009-28, 2009.

[2]M . Green, S. Hohenberger and B. Waters, ”Outsourcing the Decryption of ABE Ciphertexts,” in Proc. USENIX SecuritySymp., San Francisco, CA, USA, 2011.

[3]J. Lai, R. H. Deng, C. Guan and J. Weng, ”Attribute-Based Encryption with Verifiable Outsourced Decryption,” in Proc. IEEE Transactions on information forensics and security, vol.8, NO. 8, pp.1343-1354, 2013.

[4]A. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[5]B. Waters,”Ciphertext-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization,” in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.

[6]B. Parno, M . Raykova and V. Vaikuntanathan, ”How to Delegate and Verify in Public: verifiable co mputation from attribute-based encryption,” in Proc. TCC, pp.422-439, Springer-Verlag Berlin, Heidelberg, 2012.

[7]S. Yamada, N. Attrapadung and B. Santoso,”Verifiable Predicate Encryption and Applications to CCA Security and

Anonymous Predicate Authentication," in Proc. PKC, pp.243-261,
[8]Springer-Verlag Berlin, Heidelberg, 2012.J. Han, W. Susilo, Y. Mu and J. Yan, "Privacy -Preserving Decentralized Key-Policy Attribute-Based Encryption," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012.
[9]S. Garg, C. Gentry, S. Halevi, A. Sahai and B. Waters, "Attribute -Based Encryption for Circuits fro m Multilinear Maps," in Proc. CRYPTO, pp.479-499, Springer-Verlag Berlin, Heidelberg, 2013. [10]S. Go rbunov, V. Vaikuntanathan and H. Wee, "Attribute -Based Encryption for Circu its," in Proc. STOC, pp.545-554, ACM New York, NY, USA, 2013.